

Fonctionnement d'un ANTI-VIRUS

Présentation des principales techniques utilisées par les Antivirus pour combattre leur raison de vivre.

- Principales techniques de recherche virus

Quatre techniques majoritairement utilisées par les Antivirus, pour localiser les virus, seront présentées. Il s'agit du scanning, du moniteur de comportement, du contrôleur d'intégrité et de la recherche heuristique. Brièvement présenté, le scanneur recherche dans tous les fichiers ou en RAM un code spécifique qui est censé indiquer la présence d'un virus. Le moniteur de comportement surveille les actions habituellement menées par les virus, les contrôleurs d'intégrité signalent les changements intervenus dans les fichiers et enfin la recherche heuristique recherche des instructions généralement utilisées par les virus.

- Recherche de la signature

On nomme ça aussi scanning. C'est la méthode la plus ancienne et la plus utilisée. Son avantage est qu'elle permet de détecter les virus avant leur exécution en mémoire. Son principe est de rechercher sur le disque dur toute chaîne de caractères identifiée comme appartenant à un virus. Cependant comme chaque virus a sa propre signature, il faut, pour le détecter avec un scanneur que le concepteur de Antivirus ait déjà été confronté au virus en question et l'ait intégré à une base de données. Un scanneur n'est donc pas en mesure de détecter les nouveaux virus ou les virus polymorphes (car ceci changent de signature à chaque répliation) . Cette méthode est à la fois la plus simple à programmer mais aussi la plus longue à mettre en oeuvre car elle n'est utile que si elle recense tous les virus existants. Cela représente une somme de travail considérable et est quasiment impossible à réaliser. C'est pour ça que les concepteurs Antivirus proposent des mises à jour de la base de données tous les mois sur leur site WEB, c'est le seul moyen pour le scanneur de détecter les nouveaux virus.

- Utilisation d'un contrôleur d'intégrité :

Schématiquement, un contrôleur d'intégrité va construire un fichier contenant les noms de tous les fichiers présents sur le disque dur auxquels sont associés quelques caractéristiques. Ces dernières peuvent prendre en compte la taille, la date et l'heure de la dernière modification ou encore un checksum (somme de contrôle) Un CRC (code de redondance cyclique), ou un algorithme de checksum avec un système de chiffrement propriétaire pourra détecter toute modification ou altération des fichiers en recalculant le checksum à chaque démarrage de l'ordinateur (si Antivirus n'est pas résident), ou dès qu'un fichier exécutable est ouvert par un programme (si Antivirus est résident); en effet si le checksum d'un programme avant et après son exécution est différent, c'est qu'un virus a modifié le fichier en question, l'utilisateur en est donc informé. D'autre part Antivirus peut aussi stocker la date et la taille de chaque fichier exécutable dans une base de données, et tester les modifications éventuelles au cours du temps. Il est en effet rare de modifier la taille ou la date d'un fichier exécutable. La parade pour les virus est de sauvegarder la date du fichier avant la modification et de la rétablir après.

- Moniteur de comportement

Les moniteurs de comportement ont pour rôle d'observer l'ordinateur à la recherche de toute activité de type virale, et dans ce cas de prévenir l'utilisateur. Typiquement, un moniteur de comportement est un programme résident que l'utilisateur charge à partir du fichier AUTOEXEC.BAT. et qui reste actif en arrière plan, surveillant tout comportement inhabituel. Que va faire le zouave ? Description d'attaque virale. Les tentatives d'ouverture en lecture/écriture des fichiers exécutables. Les tentatives d'écriture sur les secteurs de partitions et de démarrage. Les tentatives pour devenir résident.

- Démarche heuristique

Fondamentalement, l'analyse heuristique concerne la recherche de code correspondant à des fonctions virales. Elle est différente dans son principe, d'un moniteur de comportement qui surveille des programmes ayant une action de type virale. L'analyse heuristique est comme le scanning, passive. Elle considère le code comme une simple donnée, et n'autorise jamais son jamais son exécution.

Une analyse heuristique va donc rechercher du code dont l'action est suspecte s'il vient à être exécuté. L'analyse heuristique permet par exemple, pour les virus polymorphes de chercher une routine de déchiffrement. En effet, une routine de déchiffrement consiste à parcourir le code pour ensuite la modifier. Ainsi lors de l'analyse heuristique, Antivirus essaie de rechercher non pas des séquences fixes d'instructions spécifiques au virus mais un type d'instruction présent sous quelque forme que ce soit. Pour en revenir à notre exemple de virus polymorphes, Antivirus cherche une suite d'instructions de lecture suivie d'une suite d'instruction d'écriture. Cette méthode est donc un peu plus intelligente que les autres : car elle vise à analyser les fonctions et instructions les plus souvent présentes et que l'on retrouve dans la majorité des virus. Cette méthode permet ainsi, contrairement au scanning, de détecter des nouveaux virus dont la signature n'a pas été ajoutée à la base de données.

- Analyse spectrale

Tout code généré automatiquement est supposé contenir des signes révélateurs du compilateur utilisé. De même, au contraire, il est impossible de retrouver dans un vrai programme exécutable compilé certaines séquences de code. C'est grâce à ce principe qu'entre en jeu l'analyse spectrale. Cette analyse vise à repérer les virus polymorphes qui sont indétectables autrement (leur signature changeant à chaque réplication). En effet, lorsqu'un virus polymorphe crypte son code, la séquence en résultant contient certaines associations d'instructions que l'on ne trouve pas en temps normal ; c'est ce que va détecter l'analyse spectrale. Par exemple, si dans un programme exécutable, Antivirus trouve une instruction de lecture d'un octet au-delà de la taille limite de la mémoire, on sera probablement en présence de code crypté, donc d'un virus polymorphe.

- Techniques d'éradication de virus

Une fois un virus détecté, que ce soit en mémoire ou sur le disque dur, il reste à le supprimer. Une fonction primordiale des Antivirus est donc la suppression des virus. Leur but est de débarrasser l'utilisateur de ce programme malveillant. Mais il n'est pas si simple que l'on croit de les éradiquer et de récupérer le programme original. En effet cela est impossible dans le cas de virus avec recouvrement : ils détruisent une partie du programme sain lors de sa duplication. La seule solution est la destruction des fichiers infectés ou carrément le formatage du disque dur. Pour les autres, même si ce n'est pas irréalisable, la tâche est cependant très ardue : il faut savoir très précisément où est

localisé, dans le fichier, le virus en question sachant qu'il peut être composé de plusieurs parties, ensuite il faut le supprimer, et enfin aller chercher la partie du programme dont le virus avait pris la place et la restaurer. Toutes ces manipulations nécessitent une connaissance parfaite du virus et de son mode d'action. Cette éradication se faisant par une recherche (du virus, de la partie déplacée), toutes les caractéristiques des différents virus doivent être répertoriées dans une base de données mise à jour pratiquement quotidiennement.

**Source : CERT/TCC
Computer Emergency Response Team / Tunisian Coordination Center
Agence Nationale de la Sécurité Informatique
Ministère des Technologies de la Communication**